WHAT IS CLAIMED IS:

1. A system comprising:

a target;

a probe operable to execute in the target and collect a predetermined set of data associated with the target; and

a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered.

2. The system, as set forth in claim 1, wherein the probe is resident in the target.

3. The system, as set forth in claim 1, wherein the monitor is operable to send the probe to the target for execution.

4. The system, as set forth in claim 1, wherein the probe repeatedly executes and the predetermined set of data varies for each execution of the probe.

5. The system, as set forth in claim 1, wherein the predetermined set of data includes system attributes and system usage data.

6. The system, as set forth in claim 1, wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe.

7. The system, as set forth in claim 1, wherein the monitor is operable to compare the calculated signature value to an expected signature value.

8. The system, as set forth in claim 1, wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe.

9. The system, as set forth in claim 1, wherein the probe is operable to generate an encryption key from the signature value for encrypting the collected predetermined set of data.

10. A method comprising:

executing a probe in a target;

collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered.

11. The method, as set forth in claim 10, further comprising receiving a request to execute the probe resident in the target.

12. The method, as set forth in claim 10, further comprising receiving the probe and executing the received probe in the target.

13. The method, as set forth in claim 10, wherein the step of executing a probe is repeated.

14. The method, as set forth in claim 10, wherein the step of executing a probe comprises collecting a different predetermined set of data for each execution of the probe.

15. The method, as set forth in claim 10, further comprising calculating a signature value of at least a portion of the probe for comparison to an expected signature value.

16. The method, as set forth in claim 10, further comprising calculating a signature value of the probe for comparison to an expected signature value.

17. The method, as set forth in claim 16, further comprising:

generating an encryption key from the signature value; and

encrypting the collected predetermined set of data with the encryption key.

18. The method, as set forth in claim 17, further comprising:

sending the encrypted data to a monitor, the data including system attribute data and system usage data;

decrypting the encrypted data using a decryption key;

verifying the system attribute data; and

generating billing data based on the system usage data in response to the system attribute data being verified.

19. A method comprising:

initiating the execution of a probe in a target;

receiving from the probe a predetermined set of data associated with the target; and

comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered.

20. The method, as set forth in claim 19, further comprising sending a request to the probe resident in the target to initiate the execution.

21. The method, as set forth in claim 19, further comprising sending the probe and executing the probe in the target.

22. The method, as set forth in claim 19, wherein initiating the execution of a probe comprises repeating execution of the probe.

23. The method, as set forth in claim 19, wherein initiating the execution of a probe comprises collecting a different predetermined set of data for each execution of the probe.

24. The method, as set forth in claim 19, further comprising:

receiving collected data encrypted by the probe using an encryption key derived from a self-hash value, the data including system attribute data and system usage data;

decrypting the encrypted data; and

verifying the system attribute data.

25. The method, as set forth in claim 23, further comprising generating billing data based on the system usage data in response to the system attribute data being verified.

26. The method, as set forth in claim 19, further comprising:

receiving a reply containing at least the collected predetermined set of data, the data including system attribute data and system usage data; and

verifying the system attribute data.